REMARKS

Applicant respectfully requests that the amendments previously submitted in response to the final office action dated August 25, 2005 not be entered.

As reflected in the above amendments, applicant intends to cancel claims 75-76 and 99-100 and incorporate their limitations into independent claims 53 and 77 respectively. However, for clarity in these remarks, applicant will first address the patentability of claims 75 and 76. The following remarks regarding claims 75 and 76 are equally applicable to claims 99 and 100.

As previously presented, claim 75 contained multiple uses of the term "instruction set" and specifically the limitation of "the third instruction set". However, the term "third" was used in error and applicant intended to recite "the *first* instruction set". Additionally, to avoid any potential confusion, applicant now proposes that the term "instruction set" should be replaced with the phrase "set of operations" which has clear support in the specification. Therefore, the subject matter of claim 75 should be amended to replace:

> "wherein the network connection device has a first instruction set, the method further comprises, prior to step (a), instantiating a virtual machine on the network connection device, the virtual machine has a second instruction set, the second instruction set is a sub-set of the third instruction set, and steps (a) through (h) are managed by the virtual machine"

with:

> "wherein the network connection device has a first ~~instruction set,~~ set of operations, the method further comprises, prior to

15

step (a), instantiating a virtual machine on the network

connection device, the virtual machine has a second ~~instruction~~

~~set,~~ set of operations, the second ~~instruction set~~ set of

operations is a sub-set of the ~~third instruction set,~~ first set

of operations, and steps (a) through (h) are managed by the

virtual machine".

Applicant submits that the subject matter of claim 77, if so

corrected, would be patentable. This correction is therefore reflected

in the amendments to claim 53.

As previously presented, claim 76 included the limitation of

receiving a pre-compiled file containing the information necessary to

manage the network traffic. In light of the amendments to the subject

matter of claim 75, discussed above, applicant submits that the

subject matter of claims 76 is also patentable.

In the Advisory Action mailed December 19, 2005, the examiner has

interpreted applicant's previous remarks to assert that the "'second

instruction set' is the rule program 66 described in the

specification". Respectfully, applicant submits that the examiner has

misinterpreted applicant's position. Applicant agrees with the

examiner's interpretation of the "second instruction set" (now the

"second set of operations") as describing a characteristic of the

virtual machine. However, applicant sees no reason why the second set

of operations being a characteristic of the virtual machine prevents

the second set of operations from being listed in the rule program.

Applicant has added dependent claim 101 (and 102) to specify that the

second set of operations is listed in the rule program in addition to

being a characteristic of the virtual machine as specified in claim 53

(and 77).

16

Page 19 of the specification states that the "rule program 66 comprises a set of operations" which means the rule program includes a set of operations, but does not mean that the rule program is exclusively limited to being a set of operations. Referring to FIG. 9, an operations file (62) and a rule file (64) are compiled to create the rule program (66). The operations file (62) "describes operations supported by components of a particular network device" (Specification, page 19, lines 10-11). When the rule program is compiled, an executable file is created that may be described as containing a list of rules for the virtual machine to implement in managing network traffic. In addition to the rules, the rule program also identifies which operations supported by the virtual machine should be used to implement each rule in the list of rules. This is so, prior to execution of the rule program by the virtual machine, a check (FIG. 11, 88) can be performed to ensure that all of the operations in the rule program correspond to registered operations of components of the virtual machine (for instance, to ensure that the correct operations file was used in creating the rule program).

The present invention, as defined by amended claim 53, thus relates to a method of managing network traffic (designated 16 in the embodiment shown in FIG. 1) being routed through a network connection device (designated 12). The network connection device includes a first set of operations. The network traffic (16) is composed of at least first and second traffic flows and each traffic flow is composed of at least one data packet (in the embodiment shown in FIG. 1, the first traffic flow is composed of packets A and the second traffic flow is composed of packets B). The method includes instantiating a virtual machine (10) on the network connection device (12) for managing the subsequent steps of the method using a second set of operations, which

17

is a sub-set of the first set of operations (see above). The method also includes receiving rule program (66) at the network connection device (12). The rule program (66) contains at least a first criterion (18), a second criterion (18), and first and second instructions (POLICY 1 and POLICY 2 respectively, FIG. 4) at the network connection device. The network connection device (12) uses the first criterion (18) to identify the traffic flow to which a data packet belongs. The network connection device (12) uses the second criterion (18) to classify a traffic flow as belonging to one of at least first and second traffic flow classes. The first and second instructions are used for processing a data packet and are associated with the first and second flow classes respectively. The method also comprises receiving a first data packet (29) that belongs to the first traffic flow at the network connection device, determining that the first data packet belongs to the first traffic flow, determining the traffic flow class to which the first traffic flow belongs, and processing the data packet according to the instructions associated with the flow class to which the first traffic flow belongs.

Hawkinson, previously cited by the examiner in regards to claim 53, describes a method for classifying information received by a communications system. Hawkinson's FIG. 2 illustrates a queuing module 200 implemented on a communications device 100 (FIG. 1). Network traffic elements, including ATM cells, are received by a receive module. Certain types of ATM cells, relating to flow control, are passed to a resource manager block 222. The resource manager 222 responds to these cells by issuing requests for establishing, terminating, and modifying connections to a connection management task 226. The connection management task 226 then directs the resource manager 222 to install, de-install, or modify the connections

18

(Hawkinson, Col. 6, lines 41 - 46). The resource manager 222 also maps class and policy definitions, such as resource requirements, for the flows. A flow database 224 containing the current resource state and other parameters and state variables is coupled to the resource manager 222 (Hawkinson, Col. 7, lines 4-10).

The receive module includes a flow classification and routing block 218 (FIG. 4). The flow classification and routing block 218 examines incoming data units and determines if the data units belong to an existing flow. If so, the flow classification and routing block then establishes the class of network traffic the existing flow belongs to using a class definition table 332 (see Table 1), a policy definition table 334 (see Table 2) and a pipe definition table 336 (see Table 3). These tables instruct the flow classification and routing block 218 how to proceed in handling the data unit. If a new flow needs to be established, the flow classification and routing block will pass a resource request to a fly-by flow admission block 232. The fly-by flow admission block in turn determines the quality of service (QoS) the new flow will require and makes a request to the resource manager 222. The resource manager 222 then determines if there are enough resources available to meet the requested QoS. If the necessary resources are available, the resource manager 222 notifies the fly-by flow admission block 232, which in turn acquires the new flow.

The present invention, as defined by amended claim 53, is distinct from the method described in Hawkinson. The method of claim 53 instantiates a virtual machine to manage network traffic being received by the network connection device. A virtual machine is a software emulation of one hardware device on another hardware device. The operations a virtual machine is capable of performing are limited

19

by i) the operations the hosting hardware device is capable of performing and ii) the degree to which the virtual machine's creator wishes to give the virtual machine access to the operations of the hosting hardware device. There is no technical reason why a virtual machine could not be instantiated on a network connection device such that the virtual machine has access to all of the network connection device's available instructions (i.e. the first set of operations). In accordance with the present invention however, the virtual machine is limited to performing actions using only operations contained within the second set of operations. Limiting the access to a sub-set of the available instructions (i.e. the second set of operations) is an intentional and significant limitation on the present invention, as defined by claim 53. Hawkinson does not disclose or suggest that the queuing module 200 is a virtual machine within the meaning of claim 53. Further, there is no disclosure, either explicitly or implicitly, that the queuing module 200 is subject to any limitation with regard to available operations of the communication device 100.

The limited number of operations available to the virtual machine is an important security feature of the present invention, as defined by claim 53. As an example, consider two network users who are exchanging confidential communications over a network. Using the method described by Hawkinson, there is nothing to prevent a third party from accessing the queuing module 200 and modifying the policy definition table 334 associated with the PDUs of the confidential communications. This could allow the third party to intercept the confidential communications. In contrast, using the present invention, as defined by claim 53, the operations of the network connection device (12) that would permit the communications to be re-routed can

20

be explicitly excluded from the second set of operations thereby making the confidential communications more secure.

In view of the above arguments, applicant submits claim 53 is patentable. It follows that dependent claims 54-74 and 101 are also patentable.
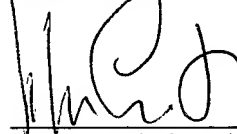
Applicant further submits that the above arguments relating to claim 53 apply equally to amended claim 77, which has been amended to incorporate the limitations of claims 99 and 100 similarly to amended claim 53 and applicant submits that claim 77 is therefore patentable. It follows that claims 78-98 and 102 are also patentable.

Regarding claims 55 and 79, applicant had included the limitation "the second section being non-exclusive of the first section" to avoid the inference that the first and second sections are exclusive of one another and to show that the second section may contain all, some or none of the elements of the first section, e.g. if the first data packet contains elements A, B, C, and D and the first section is made up of elements A and B, applicant does not intend the second section to be limited to elements C and/or D. Applicant proposes amending claims 55 and 79 to replace the potentially unclear wording above with "wherein the second section may include at least part of the first section." Applicant submits that amended claims 55 and 79 are patentable.

New independent claims 103 and 104, similar to claims 53 and 77 respectively, have been added which emphasize a different approach to

defining the present invention based upon page 19, lines 19-21 and page 22, lines 4-13.

Respectfully submitted,

John Smith-Hill
Reg. No. 27,730

SMITH-HILL & BEDELL, P.C.
16100 N.W. Cornell Road, Suite 220
Beaverton, Oregon 97006

Tel. (503) 574-3100
Fax (503) 574-3197
Docket: TUT 3094
Postcard: 12/05-32

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on the ___27th___ day of ___December___, 2005.